Publication: Mercury, Network
Date: Wednesday, February 06, 2019
Page: 8

SECURITY

Small businesses not exempt from cyber attacks

ELAINE WANG

THE threat of cyber attacks has been at the forefront of discussions in the media and in the technology industry itself over the past two years.

However, small businesses still seem to think there is little need for cyber security as they're not as lucrative targets to hackers as larger corporations are. This is entirely false.

Small and medium-sized businesses experience slightly more data breaches involving personal information and the size of data breaches are usually larger.

Data has value to hackers because it has value to a business, so no matter the size of an organisation, preparation is key.

Businesses need to start taking a holistic approach to cyber security in the workplace, taking both preventative as well as disaster recovery measures into account.

Here are some tips to help small and medium-sized businesses improve their network security.

PREVENTION

Training: User training and monitoring is extremely important as users are often the weak point of a network. Employees are usually unable to detect a fraudulent email, so companies need to educate them on spotting malware, phishing attacks and social engineering tactics to avoid accidental breaches.

User policy changes: Implementing policies that limit users' ability to install unauthorised software on work devices and requiring users to update passwords regularly can go a long way in protecting the network of a business. Requesting that users employ a mobile security tool trusted by the organisation can also help.

Network security tools: There are many monitoring and anti-malware tools on the market which can help business to protect their network. These include mobile device management, such as Microsoft 365 and Gravityzone Advanced Business Security.

Consistent security updates: A company's IT division should routinely perform software upgrades to ensure the latest security patches are rolled out across the entire organisation.

DISASTER RECOVERY

Incident response plan: A disaster recovery system for business-critical applications is crucial to minimising downtime as a result of an attack and should take into account all possible risks and what your business needs to continue operating.

Back-up systems: Implementing a robust back-up system can help to ensure that there is no loss of data which can cost the business money as well as its reputation.

An increasingly popular way of backing up important data is to use a cloud-based offering which can do this automatically.

Cyber security breaches can close a business down permanently – and in this day and age, it's not a matter of if it happens, but when.

Wang is the director of Rectron Cloud and Software Solutions